(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 940 675 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.09.1999 Bulletin 1999/36

(51) Int. Cl.[6]: **G01N 30/00**, H04L 9/32, H04L 9/00

(21) Application number: **98830118.0**

(22) Date of filing: **06.03.1998**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant:
STMicroelectronics S.r.l.
20041 Agrate Brianza (Milano) (IT)

(72) Inventors:
- **Occhipinti, Luigi**
  97100 Ragusa (IT)
- **Di Bernardo, Giovanni**
  95030 Mascalucia (IT)
- **Di Cola, Eusebio**
  98124 Messina (IT)
- **Caponetto, Riccardo**
  95100 Catania (IT)

(74) Representative:
Cerbaro, Elena, Dr. et al
STUDIO TORTA S.r.l.,
Via Viotti, 9
10121 Torino (IT)

(54) Method and system for authentication and electronic signature

(57) The method for authentication and electronic signature is of the private-key, challenge and response type between a user requesting an authorisation (for a specific transaction, or for access to particular resources), via, for example, a smart card (1) and a controller -check terminal (2)-supplying the authorisation. To increase security of the authorisation or authentication operations, the smart card (1) comprises a chaotic generator (23) generating user's acknowledgement code, which is compared with a comparison code generated by the check terminal (2) using a chaotic generator (30) which is the same.

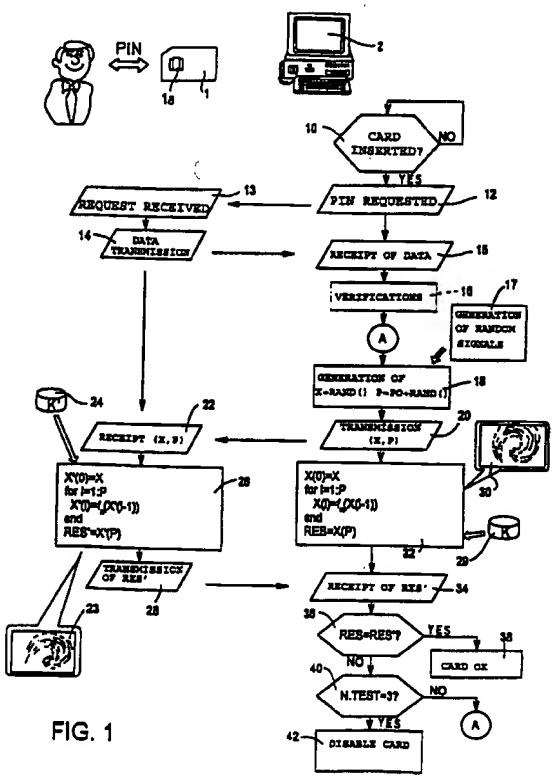


FIG. 1

EP 0 940 675 A1

Description

[0001] The present invention relates to a method and system for authentication and electronic signature.

[0002] In the modern theory of cryptographic techniques, a fundamental part is played by systems and methodologies for authentication of the user (sender or recipient), or of the message, and of certification of the authenticity of the data (electronic signature), to protect the exchange of data on channels that are publicly accessible, against active attacks aimed at detracting from integrity of an original message, with the possibility of a non-authorised third party interacting directly with the sender and/or recipient parties. The purpose of these systems is to prevent a communication channel, which is mistakenly thought to be secure, from being used for unplanned or undesirable purposes (undesirable execution of transactions and drawing up of contracts, acts of intimidation, computer piracy or terrorism, or acquisition of selective access data, for example relating to payment).

[0003] A problem of this type is all the more serious, the more the mechanism for handling the data can be kept concealed from one party or the other: the extent of the damage caused by an active attack is far greater than that caused by a passive attack, in which the pirate user simply listens to, and deciphers data considered secret, and is transmitted in cryptographic form on a channel.

[0004] Furthermore, it has been found in the last few years that by using ever more powerful computing means or distributed computer resources, successful attacks have been made on the most powerful cryptography algorithms now in existence, such as DES, which until a few years ago were considered impossible to "crack".

[0005] Within the context of known authentication systems, use is frequently made of "challenge and response" authentication methods that have a private key (secret-type cryptographic algorithm), which is known only to the two parties which want to communicate. In these methods, one of the two parties generates a random number, which is also supplied to the other party, both parties compute independently, and each uses its respective private key and the random number generated, and this code is then compared with the code calculated by the other party, to verify the authorisation and access to specific resources and/or to authenticate a message sent with the acknowledgement code.

[0006] As is known, in an authentication system of this type, the security of the system itself, i.e. the probability of a pirate user finding the key that opens the entire system, once the authentication system is known to everyone, is associated with the following factors:

1) secrecy of the key;
2) statistical incidence of the key in the coded message, i.e. to what extent the statistical distribution of the symbols in the key can detract from the security of the system (this is the case of cryptographic systems in which the user is asked to select the cryptographic key; here there is a high probability that words which make complete sense will be used, with statistical incidence of each symbol that is typical of the language or vocabulary used, to the detriment of the security of the algorithm itself and the cryptographic key);
3) pseudo-random distribution of the symbols in the coded text, i.e. index of coincidence of each symbol that is as small as possible, according to the Friedman test or K-test (the typical case of a cryptographic system which does not comply with this principle, and is therefore easy to attack, is Vigènere's cipher);
4) statistical recurrence of the maps of correspondence between a text or portion of text written out in full, and the corresponding text in coded form.

[0007] The object of the invention is thus to provide a method of the challenge and response type that has an improved level of security compared with the known methods, as far as the above-described criteria 2) - 4) are concerned.

[0008] According to the present invention, a method, an integrated circuit and a system for authentication and electronic signature are provided, as defined respectively in claims 1, 2, 10 and 16.

[0009] For better understanding of the present invention, two preferred embodiments are now described, purely by way of non-limiting example, with reference to the attached drawings, in which:

- figure 1 shows a block diagram relating to a first embodiment of the present method;
- figure 2 is a bifurcation diagram for a chaotic generator used according to the method of figure 1;
- figure 3 shows a block diagram relating to a second embodiment of the present method;
- figure 4 shows a block diagram relating to the method of figure 3;
- figure 5 shows a block diagram relating to circuit architecture for implementation of the present method;

- figure 6 shows the block diagram of a component of figure 5;
- figure 7 shows the state diagram of one of the blocks of figure 6;
- figure 8 shows the internal architecture of another block of figure 6; and
- figure 9 shows a different embodiment of the block of figure 8.

[0010] Hereinafter a method and a system are described for authentication and electronic signature of the private-key, challenge and response type between at least two parties, i.e. a user who requests an authorisation (for a specific transaction, or for access to particular resources), or who sends an authenticated message, and a controller which supplies the authorisation or checks the authenticity of the message received. For example, the user can operate by means of a "smart card", and interact with a check terminal or a remote controller, via an interface terminal. To increase the security of the operations of authorisation or authentication, the system described uses a chaotic generator for generation of the user's acknowledgement code or signature.

[0011] In this specification, the term "chaotic generator" means a non-linear dynamic circuit with chaotic development, which is extremely sensitive to its initial conditions, such that the signals generated from two initial conditions which are as close as required to one another, tend very quickly to diverge, and over a period of time develop in a manner which is altogether uncorrelated to one another. As is known, the typical development of a chaotic signal resembles a random signal, the value of which at the moment $t+\Delta t$ is all the more unforeseeable at the moment t, the greater Δt. From the statistical point of view also, a chaotic process is by nature a non-stationary, and in particular it is a non-periodic process, such that its frequency content continually changes its distribution ("randomness"). Thereby, the generator of the chaotic signal used for acknowledgement cannot be identified simply by observation of a high number of exchanged acknowledgement signals, even on a public network.

[0012] Figure 1 shows the flowchart for the authentication method of a smart card 1 including an integrated circuit 1a to allow access to data and/or resources of a system via a gate comprising a check terminal 2. The card 1 and the check terminal 2 interact via respective input/output means, represented schematically in the figure by horizontal arrows.

[0013] In this embodiment, both the card 1 and the check terminal 2 can generate a chaotic signal internally (in a concealed manner); for this purpose they have a chaotic generator circuit (an embodiment of which will be illustrated hereinafter with reference to figures 5-8) which, on the basis of an initial condition X_0 selected randomly in an n-dimensional space, generates an output signal RES. The chaotic generators of card 1 and check terminal 2 can be programmed (in the same manner) through a series of parameters representing the cryptographic key K=K' (private or symmetrical key system).

[0014] In particular, with reference to figure 1, initially, after the check terminal 2 has detected insertion of a card 1 in an appropriate reading slot (YES output from block 10), it asks card 1 to transmit identification data, including PIN (Personal Identification Number), block 12. When card 1 receives the request (block 13), it transmits this data (block 14). After receipt of the data transmitted by card 1 (block 15) and checking the identification data (for example by asking the user for the PIN and comparing this with the PIN received from card 1) and optionally requesting the type of operations or type of access required by the user, block 16, check terminal 2 generates a signal or initial datum X_0 via a random-value generation circuit 17, and also, again using circuit 17, it generates a number P greater than a minimum predetermined value P_0 and representing a development time of the chaotic generator, i.e. the number of iterations, in the case of a discrete generator (block 18).

[0015] Subsequently, check terminal 2 transmits signals of the initial datum X_0 and the development time P, both to card 1 and to its own chaotic generator, block 20. Then, card 1 receives signals X_0 and P, block 22, and transfers them to its own chaotic generator 23, which, on the basis of X_0 and P, and a secret key K' stored in a location 24 of card 1 itself, calculates an authentication code RES' using a function $f_{K'}(x)$, block 26. Card 1 then transmits authentication code RES' to check terminal 2, block 28.

[0016] After transmitting X_0 and P, check terminal 2 in turn calculates a comparison code RES, using initial datum X_0, development time P, and its own secret key K, which is stored in an appropriate location 29, via an own chaotic generator 30, implementing a function $f_K(x)$ which is the same as $f_{K'}(x)$ (block 32). For example, the secret key K used by generator 30 can be selected, on the basis of the received PIN number, from a data base or a memory having several locations, each associated in a known manner with a specific user or group of users, such that the function $f_K(X)$ is different for various users or groups of users. Then, after receiving the authentication code RES' from card 1 (block 34), check terminal 2 compares just calculated comparison code RES with authentication code RES' received from card 1 (block 36); if these codes are equal (YES output from block 36), it accepts the card and supplies an authorisation for access or for executing the required operations (block 38); if the codes are not the same (NO output from block 36), it checks whether access has already been attempted three times (block 40); if this is not true (NO output), a further attempt is made, returning to block 18, but if the result is positive (YES output), card 1 is disabled by disabling the PIN

identification number (block 42), as already happens for most access control systems.

[0017] The above-described method has the following advantages. Firstly, use of chaotic generators with a key allows the user, by means of his card, via the authentication code, to supply a response (or a series of responses), which is completely unpredictable for an external observer from the interrogation which the check system (terminal) generates randomly in the individual cases.

[0018] The random variation of the number of discrete instants (development time P) in which the chaotic generator is allowed to evolve ensures that even when the terminal-card system is observed for a sufficiently large number of times, an observer cannot characterise the generator even in statistical form, which, in the case in question, would allow reconstruction of the phase diagram of the generator, by characterising the specific attractor (although qualitatively).

[0019] The possibility of generating a (theoretically infinitely) high number of different keys K, by modifying radically the behaviour of the dynamic system, can easily be used during construction and parametrisation of the chaotic generator. In fact for this purpose, the infinite number of states characterising a chaotic generator near a bifurcation is exploited (as shown in figure 2 for a chaotic generator which implements the function $f_k(x)=Kx1-x$). This possibility is exploited in this specific case by using discrete words of any length, from a continuous-time, non-linear dynamic system, within an appropriate range of parameters that govern the bifurcation. In fact, by virtue of the features of chaotic systems, the continuous-time chaotic system can be discretised starting from two values of the parameters which are infinitely close to one another (i.e. which are distant by 1 less significant bit [LSB], irrespective of the word length). In suitable conditions, designed to avoid cyclicity of the wave forms generated by the discretised system and known to persons skilled in chaotic systems, two chaotic generators with parameters which may even be very similar, will produce results which are altogether different from one another when they are allowed to evolve for an appropriate time interval.

[0020] The computational complexity of this system depends substantially on the order of the digitalised chaotic generator (f_k, function), on the discretization accuracy and on the evolution time interval before giving the response, i.e. on parameters which can be adapted arbitrarily according to the security level to be achieved.

[0021] Figure 3 shows a second embodiment of the present method, relating to use as a certification and electronic signature method, in the case of a transaction between a user, an interface terminal (which acts as a card reader), and a banking system. In particular, reference is made to a case where the user, holding a card again indicated at 1, must purchase from a generic terminal 50 (with which he interacts by means of respective input/output circuits represented symbolically by oblique arrows) with reference to a banking system represented by a check processor 51 connected to terminal 50 in a known manner (for example by a dedicated line or telephone line, also represented schematically by arrows).

[0022] In detail, initially, after terminal 50 has detected insertion of a card 1 in the appropriate reading slot (YES output from block 60), it asks card 1 to transmit the identification data (PIN), block 62. When card 1 receives the request (block 63), it transmits this data (block 64). After receiving the data transmitted by card 1 (block 65), terminal 50 communicates to the user the data relating to the transaction (payment amount), and asks the user to enter the PIN, block 66; as soon as terminal 50 receives the PIN from the user, it compares it with the PIN received from the card 1 for user certification, in a known manner, indicated in the figure by self-certification block 68. Terminal 50 then composes a message M to be transmitted to check processor 51 (block 70), and to which an electronic signature must be added. In particular, message M comprises identification number of the terminal itself POS_ID, date, payment amount, any predetermined data or information associated with terminal 50, and PIN. The message is associated with a random number generated by a random number generator 71, which number represents the development time of the chaotic generator, i.e. the number of iterations, in the case of a discrete generator. Message M is preferably divided into blocks X_j, each accompanied by a respective random number P_j. Then, block 72, terminal 50 supplies card 1 with the message blocks (X_j, P_j).

[0023] After receiving blocks X_j and respective random numbers P_j, block 74, card 1 transfers them one at a time to its own chaotic generator 23, which, on the basis of a function $f_{k'}(X)$ using a secret key K' stored in location 24 of card 1, on the basis of the preceding calculation result (CERT'), calculates a new result (CERT'), block 76, for each block X_j, and carries out P_j iterations, as shown schematically with reference to figure 4.

[0024] In figure 4, message M comprises a plurality of message blocks $X_1, X_2, ..., X_m$, supplied in succession to a first input of a node 97 defining an arithmetic operator (for example an EXOR). The output of node 97 is supplied to a generator block 98 including chaotic generator 23, or the chaotic generator associated with check processor 51 and implementing function $f_k(x)$; for each message block M, the respective value P_j is also supplied to generator block 98; the output of generator block 98 thus supplies value CERT, and is connected to a second input of node 97. At each j-th iteration, when a new message block X_j arrives, generator block 98 is then supplied, as an initial value, with the sum of message block X_j and final signal CERT calculated in the previous iteration, and generator block 98 calculates a new value CERT, by applying function $f_{k'}(x)$ for a number of times equal to P_j; the final result (after processing of the m-th message block X_m) defines the electronic signature.

[0025] With reference again to figure 3, when all message blocks have been processed, card 1 sends electronic signature CERT' to terminal 50, block 78.

[0026] When terminal 50 receives the electronic signature CERT' (block 80), it composes the original message

(formed by blocks X_j and respective random numbers P_j) with the electronic signature CERT' (block 82), transmits them to check processor 51, and waits for confirmation from check processor 51 (block 84). When it receives the transmitted message (block 88), check processor 51, having an own chaotic generator 87, calculates an authentication signature CERT using blocks X_j, respective random numbers P_j, and its own secret key K, stored in an appropriate location 89 (block 90). At the end of calculation of the comparison signature CERT, check processor 51 compares just calculated comparison signature CERT with electronic signature CERT' received from terminal 50 (block 92); if the two signatures are equal (YES output from block 92), check processor 51 generates a confirmation message for terminal 50 (block 94), enabling it to accept the transaction; if the signatures are not the same (NO output), check processor 51 rejects the card and sends a corresponding message (block 96).

[0027] The above-described method ensures security of all components of the transaction (card 1, terminal 50, and check processor 51).

[0028] Here, recourse to chaotic generators is carried out by card 1 and check processor 51, which checks authenticity of the signature, with the same criterion adopted for authentication described with reference to figure 1, whereas terminal 50 in this case simply acts as an intermediary between user and banking system.

[0029] Signature generation from the sent message blocks and the series of time intervals generated by terminal 50 ensures that if the message were corrupted at any point of transmission, the corrupted version would not be recognised, and message itself would be rejected.

[0030] Consequently, any fraudulent attempt to modify the message would immediately be revealed, and stopped by virtue of lack of correspondence of the message with the electronic signature which accompanies it. In addition, use of a chaotic generator and a private key ensures that the electronic signature can be reconstructed only by the recipient of the message (card management centre), for the reasons already illustrated.

[0031] Hereinafter, a circuit architecture will be described for implementing the authentication and electronic signature operations, as shown in aforementioned blocks 26 and 76. Similar architecture can be implemented for blocks 32 and 90.

[0032] Figure 5 shows the block diagram implementing an integrated circuit 1a bonded to smart card 1. This diagram is however valid for other implementations in dedicated systems and architectures needing a check of user and data authenticity, for ensuring access security to a specific service, i.e. where it is necessary to verify the integrity of data and information exchanged during for example an electronic transaction operation, by providing a certificate of authenticity forming an electronic signature.

[0033] In detail, in figure 5, integrated circuit 1a comprises an I/O interface 100 for receiving data from terminal 2 or 50, and transmitting thereto the required data, including PIN and authentication code RES' or electronic signature CERT', as indicated in the figure by a 16 bit bus 103. The I/O interface 100 is connected to a cryptographic unit 101 via a two-way data bus 104 (receiving the authentication code or the electronic signature), and to a controller 102 via a 16 bit data bus 105 and a line 106, on which instructions are exchanged; a line 107 from the I/O interface 100 also supplies an external clock signal CK to cryptographic unit 101 and to controller 102.

[0034] Controller 102 is connected to a memory 110 storing data (including the PIN) of card 1 via a bus 111, and to cryptographic unit 101, for exchange of signals S, R and RD, via lines 112a, 112b.

[0035] Cryptographic unit 101 comprises a crypto-processor 113, an internal clock generator 114, a series of registers 115, and storage location 24 for the key K. In detail, internal clock generator 114 receives the external clock signal CK, and generates an internal clock signal CK1 supplied to crypto-processor 113 on a line 122. For example internal clock generator 114 may comprise a frequency multiplier, thereby internal clock signal CK1 has multiple frequency with respect to external clock signal CK. Location 24 (for example comprising 64 non-volatile memory cells and connected to controller 102 via a programming line 128 shown as a broken line), contains the programmable secret key K which is supplied to crypto-processor 113 via a 64 bit bus 123, whereas registers 115 are connected to crypto-processor 113 via a 64 bit bus 124.

[0036] Cryptographic unit 101 is located in an area of integrated circuit 1a which is concealed from the exterior, by virtue of a metal layer 127 covering circuit 1a to prevent fraudulent acquisition of stored data and structures by suitable inspection techniques.

[0037] The purpose of controller 102 is to manage flow of data between terminal 2, 50 and memory 110, data writing and updating in memory 110, programming of location 24, and to check that the operations carried out by crypto-processor 113 are synchronised with interface 100.

[0038] Figure 6 shows a block diagram of crypto-processor 113 in case of the authentication method of figure 1, and comprises a control unit 120, preferably formed by a states machine, and chaotic generator 23, implementing function $f_k(x)$. Control unit 120 and chaotic generator 23 communicate via 64 bit buses 125, 126.

[0039] Control unit 120 receives start S and reset R signals on lines 112a, signal CK1 on line 122, initial datum X_0 on 16-bit line 104a, and iteration number P on 16-bit line 104b, and supplies as output ready signal RD on line 112b and output datum OUT (corresponding to the authentication code) on 16-bit line 104c; lines 104a, 104b and 104c together form bus 104.

[0040] In particular, control unit 120 executes the algorithm shown in states diagrams of figure 7, and comprises the following states:

STATE 0: assigns "1" to RD (showing that it is available for a new operation), resets the value of register N (belonging to the group of registers 115 and representing the number of iterations carried out) and assigns value X_0 to register X (belonging to the group of registers 115), after standardisation to 64 bits. It then waits for start signal S to be activated, to progress to state 1;

STATE 1: recalls function $f_k(x)$, supplying the value of internal register X, and progresses to state 2;

STATE 2: reads the value generated by function $f_k(X)$ and supplies this value to X, increments the value of internal register N, and progresses to state 3;

STATE 3: if the value of register N is lower than P, it returns to state 1, otherwise it progresses to state 4;

STATE 4: allocates "0" to RD (indicating that it has finished the operation) and supplies the output OUT with value $f_k(x)$, after standardisation to 16 bits. It waits until signal S has been deactivated to return to STATE 0; this prevents it from restarting a new process after having terminated the current process.

[0041] If the method according to figure 3 is to be implemented, it will be appreciated that in addition to control unit 120 and chaotic generator 23, the crypto-processor 113 must also comprise a unit which activates summation node 97 of figure 4, and the algorithm of control unit 120 must be modified such as to comprise the control states of the summation node and of the iteration of the combination of the message blocks (external loop of block 76).

[0042] An embodiment of the chaotic generator 23 is shown in figure 8, in case the following function is implemented:

$$f_k(x) = K.x.(1-x) \qquad \text{where } 0<x<1 \text{ and } 3<K<4.$$

[0043] Chaotic generator 23 comprises a combinatorial logic unit including a first and a second multiplier 130, 131 and a subtractor 132. In detail, first multiplier 130 has two inputs connected to buses 123 and 125, and a (128 bit) output connected to an input of second multiplier 131; subtractor 132 has a first input also connected to bus 125, a second input receiving the value "1" and standardised to 64 bits, and a (128 bit) output connected to the second input of second multiplier 131; the output of second multiplier 131, which has 64 bits, is connected to bus 126.

[0044] Figure 9 shows a different embodiment of chaotic generator 23, implementing function $f_k(x)$ in a combined analogue-digital mode. In detail, the circuit of figure 9 comprises a digital/analogue converter 140, to the input of which (indicated at 125, by analogy with figure 8) there is supplied the initial datum X_0 or the result X of the preceding iteration, and the output of which is connected to a non-linear-type analogue circuit 142 which can be programmed digitally (via an input, again indicated as 123) which implements function $f_k(x)$; the output of analogue circuit 142 is connected to an analogue/digital converter 144 supplying at its output (again indicated as 126) the digital value corresponding to the analogue value generated by circuit 142.

[0045] In the circuit of figure 9, presence at the input and at the output of the initial datum and the result in digital form ensures that a same calculation accuracy level is obtained (to the least significant bit) both by the card 1 and by the check component (terminal 2 or processor 51), and thus ensures generation of the same acknowledgement code, starting from same initial conditions and using a same key.

[0046] In general, selection of the embodiment of the circuit implementing the function $f_k(x)$ in a purely digital manner (as in figure 8), or with a combined analogue/digital signal (figure 9), depends, in the individual cases, on the requirements in terms of circuit complexity, accuracy and sensitivity to process variations. In particular, implementation of function $f_k(x)$ in a purely digital form generally provides a high level of accuracy, and requires greater circuit complexity (owing to the presence of a larger number of transistors to implement the digital multipliers, with a consequent increase in the bulk of the device), compared with the circuit embodiment in hybrid form, shown for example in figure 9.

[0047] Finally, it is apparent that many modifications and variants can be made to the method and the architecture described and illustrated here, all of which come within the scope of the invention, as defined in the attached claims. For example, besides the described two applications, the present method can be applied to a direct transaction request from a terminal or personal computer, which includes acknowledgement code generation structures (authorisation or signature) and message generation structures, similarly to the arrangement described with reference to figure 3. In addition, improvements relating to security can be obtained by adopting complex chaos generation functions, with a higher number of parameters which form the key. These characteristics make the system very secure as far as prevention of attacks based on the statistical method are concerned.

Claims

1. A method for generating an authentication and electronic signature signal, for use in an acknowledgement and authorisation system, comprising the step of generating an authentication and electronic signature signal by using a private key, characterised in that said step of generating an authentication and electronic signature signal comprises the step of generating a chaotic signal.

2. A method for authentication and electronic signature, comprising the steps of generating an authentication and electronic signature signal by using a private key; generating a comparison signal by using a second private key equal to the first private key; and comparing said authentication and electronic signature signal with said comparison signal, characterised in that said steps of generating an authentication and electronic signature signal and generating a comparison signal comprise the step of generating a chaotic signal.

3. A method according to claim 1 or 2, characterised in that it comprises the step of acquiring an initial signal; and in that said step of generating a chaotic signal is performed on the basis of said initial signal.

4. A method according to claim 3, characterised in that said initial signal is a random signal.

5. A method according to claim 3, characterised in that said initial signal comprises a message to be transmitted.

6. A method according to claim 5, characterised in that said step of acquiring an initial signal comprises the step of acquiring a plurality of message blocks.

7. A method according to claim 6, in which said message blocks comprise at least a first message block, a successive message block and a final message block; characterised in that said step of generating a chaotic signal comprises the steps of:

   a) acquiring the first message block;
   b) generating a chaotic output signal from said first message block;
   c) combining said chaotic output signal with the successive message block to obtain a combined block;
   d) generating a new chaotic output signal from said combined block;
   e) repeating said steps c) and d) as far as the last message block; and
   f) supplying said chaotic output signal as the signature of said message.

8. A method according to any one of claims 1-6, characterised in that it further comprises the step of acquiring a random signal, and in that said step of generating a chaotic signal comprises the step of activating a chaotic generator for a development time correlated to said random signal.

9. A method according to claim 7, characterised in that it also comprises the step of acquiring a respective random signal for each message block, and in that said steps b) and d) comprise the step of activating a chaotic generator for a development time correlated to the respective random signal.

10. An integrated circuit (1a) for generating an authentication and electronic signature signal, for use in an authentication and electronic signature system, comprising a generation unit (101) for generating an authentication and electronic signature signal which uses a private key; characterised in that said generation unit (101) comprises a chaotic generator (23).

11. An integrated circuit according to claim 10, characterised in that it comprises first acquisition means (104a, 97) for acquiring an input signal, said first acquisition means being connected to an input of said chaotic generator (23; 98).

12. An integrated circuit according to claim 11, characterised in that said first acquisition means (104a, 97) comprises receiving means (104a) for receiving successive blocks of message; summing means (97) having a first input connected to an output of said respective chaotic generator (98), a second input connected to said receiving means, and an output connected to the input of said chaotic generator (98); and first iteration control means (120) for activating said summing means and said chaotic generator for each message block.

13. An integrated circuit according to any one of claims 10-12, characterised in that it comprises second acquisition

means (104b) for acquiring a random development time signal; second iteration control means (120) receiving said random development time signal and repeatedly controlling said chaotic generator (23) for a development time which is correlated to said random development time signal.

14. An integrated circuit according to claim 12, characterised in that it comprises an interface unit (100); a cryptographic unit (101) connected to said interface unit; a control processor (102) connected to said interface unit and to said cryptographic unit; and a memory unit (110) connected to said control processor; and in that said cryptographic unit (101) comprises a crypto-processor (113), a plurality of internal registers (115), and a permanent memory (24) for said private key.

15. An integrated circuit according to claim 14, characterised in that said crypto-processor (113) comprises a control unit (120) and a digital circuit (23), said control unit comprising a states machine, and said digital circuit (23) comprising said chaotic generator.

16. An authentication and electronic signature system comprising first generator means (26; 76) for generating an authentication and electronic signature signal using a first private key; second generator means (32; 90) for generating a comparison signal using a second private key equal to the first private key; and comparison means (36; 92) receiving said authentication and electronic signature signal and said comparison signal, characterised in that said first and second generator means (26; 76, 32; 90) comprise a respective chaotic generator (23, 30; 87).

17. A system according to claim 17, characterised in that it comprises a first random generator (17) supplying an initial random signal to said first and second generator means (26; 32).

18. A system according to claim 17, characterised in that it comprises a generator (70) for a message to be transmitted; and transmitter means (72, 82) subdividing said message into a plurality of message blocks, and supplying said message blocks to said first and second generator means (76, 90) as an initial signal.

19. A system according to claim 18, characterized in that said first and second generator means each comprise:

- summing means (97) having a first input connected to an output of said respective chaotic generator (98), a second input receiving a message block and an output supplying a combined block;
- first iteration control means (120) activating said summing means (97) and said chaotic generator (98) for each message block.

20. A system according to any one of claims 16 to 19, characterised in that it comprises a second random generator (71) generating a random time development signal, and in that said first and second generator means (76, 90) each comprise respective second iteration control means repeatedly controlling said respective chaotic generator (23, 87) for a development time correlated to said random time development signal.

21. A system according to any one of claims 16 to 20, characterised in that it comprises a smart card (1) and a check terminal (2) comprising respective input/output means connectable to one another, and in that said first generator means (26) belong to said smart card (1) and in that the second generator means (30) belong to said check terminal (2).

22. A system according to any one of claims 16 to 20, characterised in that it comprises a smart card (1), an interface terminal (50), and a central check unit (51), said smart card (1) and said interface terminal (50) comprising respective first input/output means connectable to one another; said interface terminal (50) and said central check unit (51) comprising respective second input/output means connected or connectable to one another; in that said first generator means (76) belong to said smart card (1) and in that the second generator means (90) belong to said check unit (51).

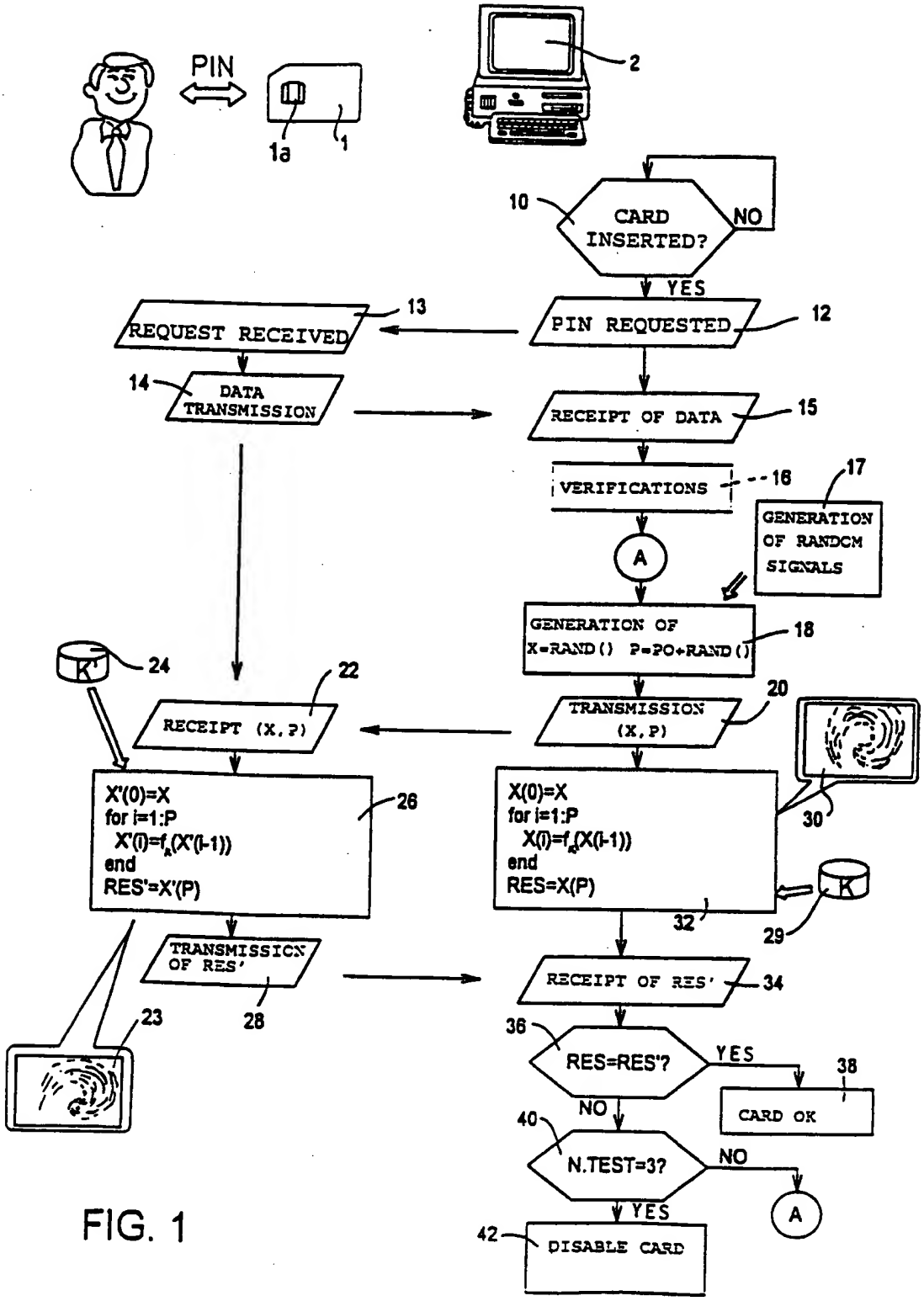

PIN
1a
1
2
10
CARD INSERTED?
NO
YES
PIN REQUESTED
12
REQUEST RECEIVED
13
14
DATA TRANSMISSION
RECEIPT OF DATA
15
VERIFICATIONS
16
17
GENERATION OF RANDOM SIGNALS
A
GENERATION OF X=RAND() P=PO+RAND()
18
24
22
RECEIPT (X,P)
TRANSMISSION (X,P)
20
X'(0)=X
for i=1:P
X'(i)=f_A(X'(i-1))
end
RES'=X'(P)
26
X(0)=X
for i=1:P
X(i)=f_A(X(i-1))
end
RES=X(P)
30
29
32
TRANSMISSION OF RES'
28
23
RECEIPT OF RES'
34
36
RES=RES'?
YES
38
CARD OK
NO
40
N.TEST=3?
NO
A
YES
42
DISABLE CARD

FIG. 1

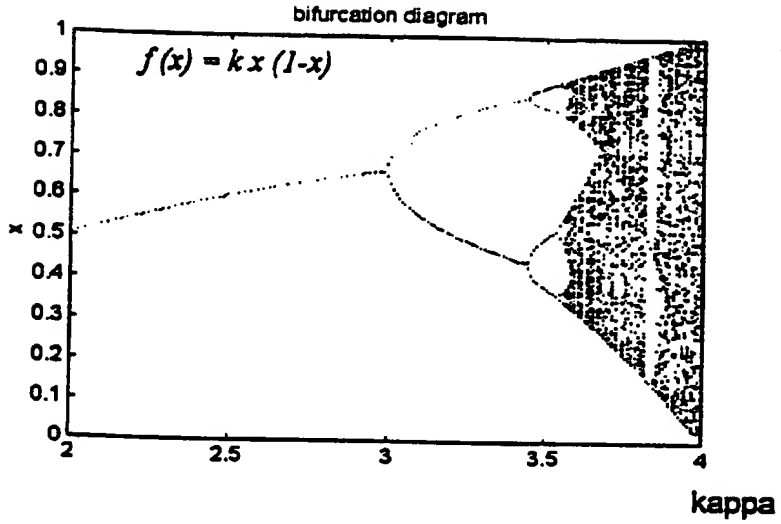


FIG. 2

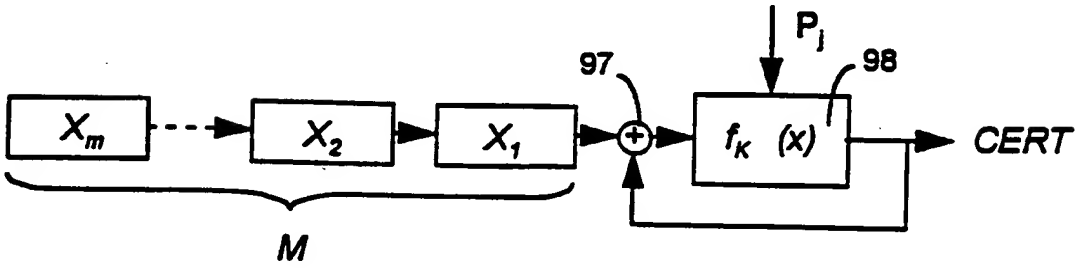


FIG. 4

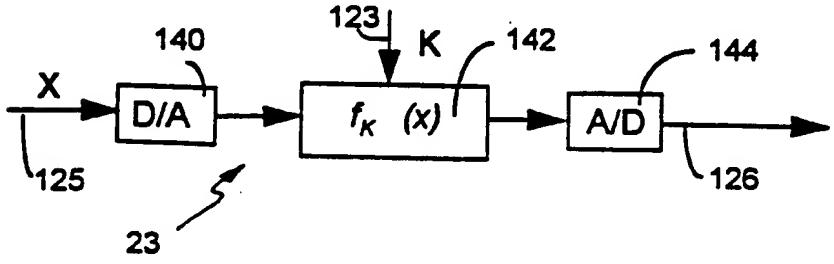


FIG. 9

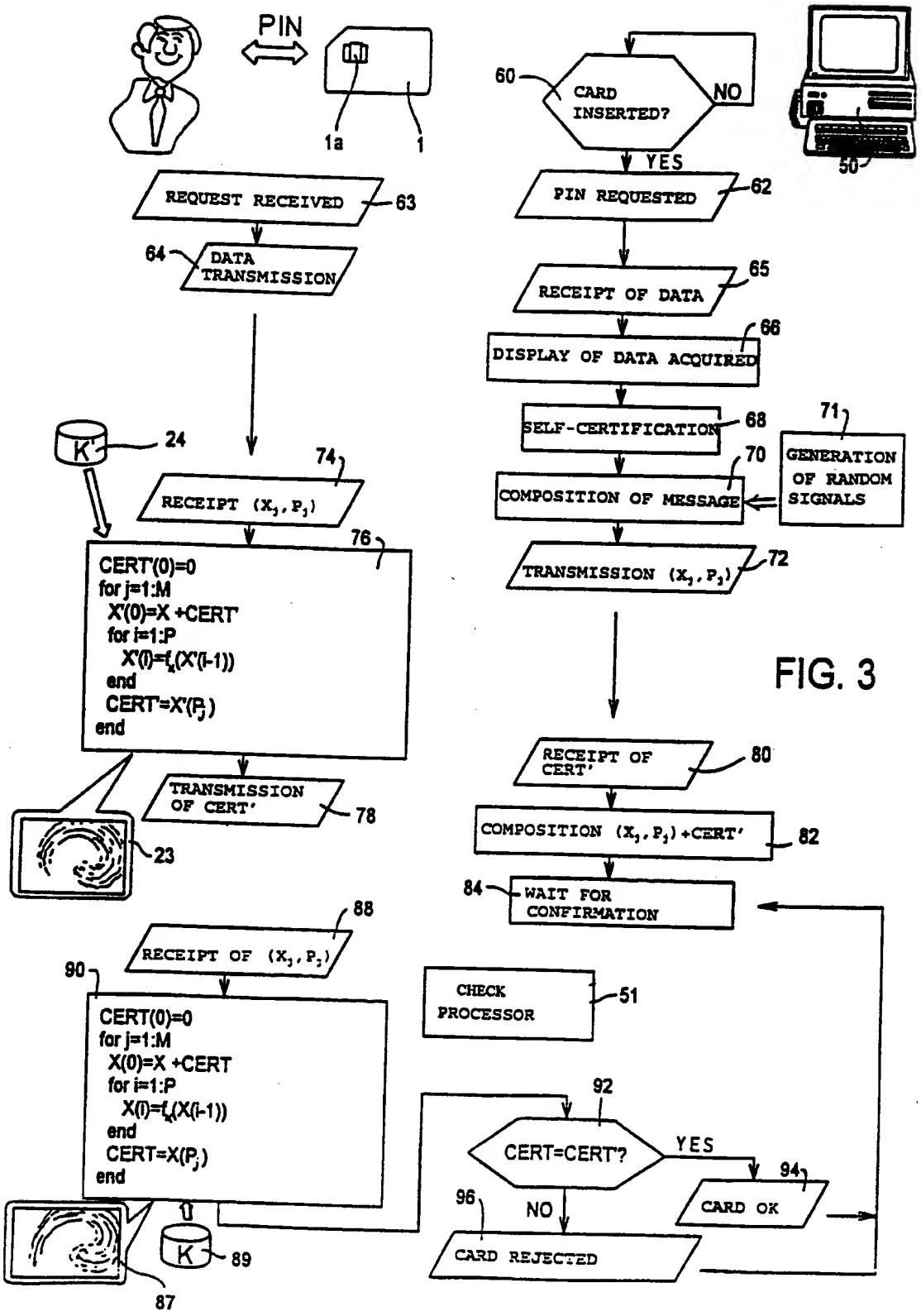
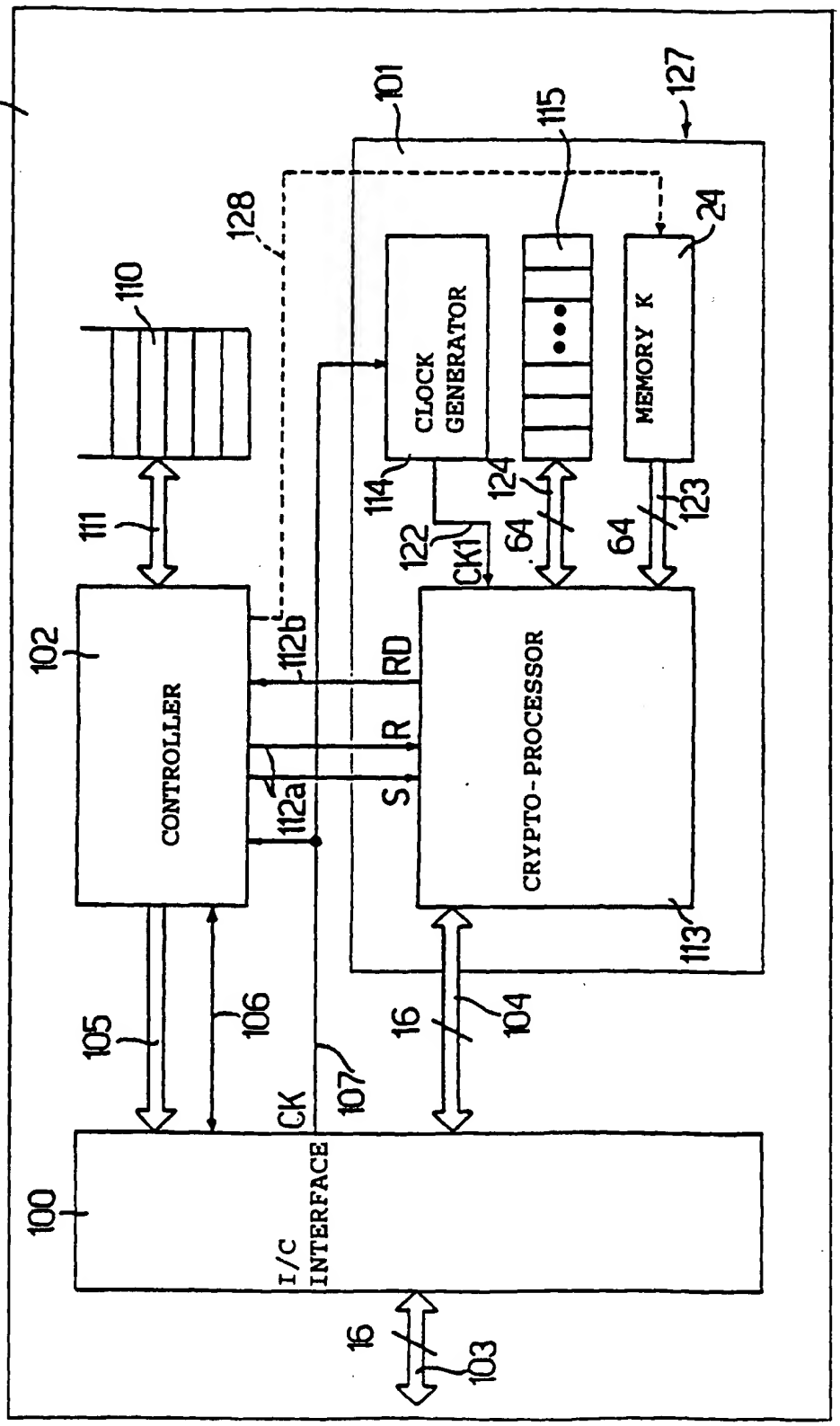

PIN
1a
1
60
CARD INSERTED?
NO
YES
50
REQUEST RECEIVED
63
PIN REQUESTED
62
64
DATA TRANSMISSION
RECEIPT OF DATA
65
66
DISPLAY OF DATA ACQUIRED
SELF-CERTIFICATION
68
71
GENERATION OF RANDOM SIGNALS
K'
24
74
RECEIPT (X_j, P_j)
70
COMPOSITION OF MESSAGE
76
CERT'(0)=0
for j=1:M
X'(0)=X +CERT'
for i=1:P
X'(i)=f_i(X'(i-1))
end
CERT'=X'(P_j)
end
TRANSMISSION (X_j, P_j)
72
TRANSMISSION OF CERT'
78
23
RECEIPT OF CERT'
80
COMPOSITION (X_j, P_j)+CERT'
82
84
WAIT FOR CONFIRMATION
88
RECEIPT OF (X_j, P_j)
90
CHECK PROCESSOR
51
CERT(0)=0
for j=1:M
X(0)=X +CERT
for i=1:P
X(i)=f_i(X(i-1))
end
CERT=X(P_j)
end
92
CERT=CERT?
YES
94
CARD OK
96
NO
CARD REJECTED
K
89
87

FIG. 3

Fig.5


1a
101
115
127
128
110
24
CLOCK GENERATOR
MEMORY K
114
124
123
122
CK1
64
64
111
102
CONTROLLER
112b
RD
R
S
112a
CRYPTO-PROCESSOR
113
105
106
16
104
CK
107
100
I/C INTERFACE
16
103

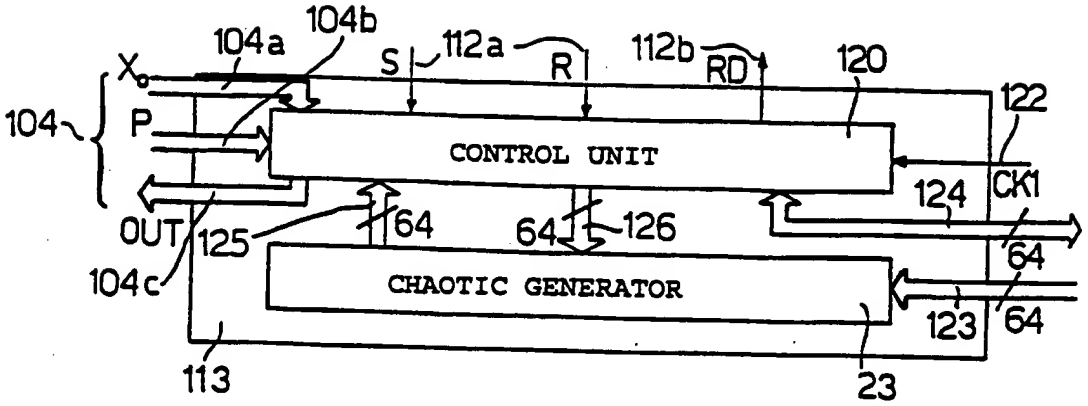


FIG. 6

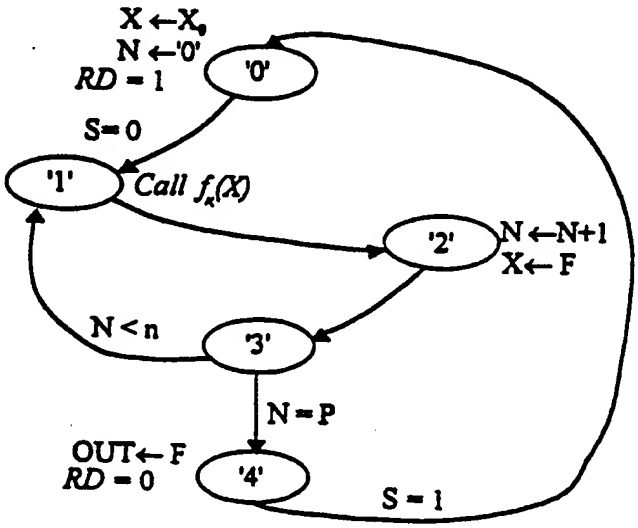


FIG. 7

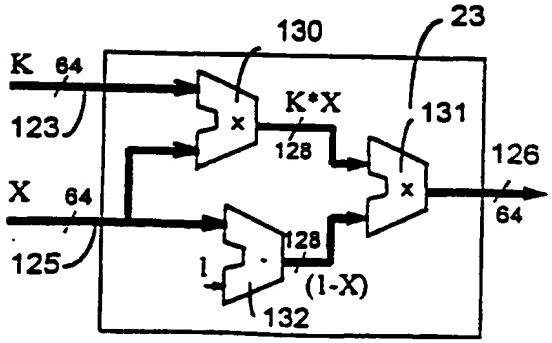


FIG. 8

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 83 0118

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X A Y	US 5 048 086 A (BIANCO ET AL.) 10 September 1991 * column 1, line 60 - column 2, line 37 * * column 6, line 18 - line 53 * * column 4, line 59 - column 5, line 24 * * abstract *	1,3,4, 10,11,14 16,17 2	G01N30/00 H04L9/32 H04L9/00
X	PATENT ABSTRACTS OF JAPAN vol. 097, no. 010, 31 October 1997 & JP 09 153014 A (WATANABE EIJI;METEOOLA SYST KK), 10 June 1997 * abstract *	1,3	
Y	HOPKINS: "Transaction Incrementing Message Authentication Key" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 26, no. 1, June 1983, pages 199-201, XP002082637 New York, US * the whole document *	2	
A	WALKER M: "SECURITY IN MOBILE AND CORDLESS TELECOMMUNICATIONS" PROCEEDINGS OF THE ANNUAL EUROPEAN CONFERENCE ON COMPUTER SYSTEMS A SOFTWARE ENGINEERING (COMPEURO), THE HAGUE, MAY 4 - 8, 1992, no. CONF. 6, 4 May 1992, pages 493-496, XP000344244 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS * page 493, right-hand column, line 1 - line 21 *	1,16	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	29 October 1998	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 83 0118

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

29-10-1998

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5048086 A	10-09-1991	DE 69118977 D	30-05-1996
		DE 69118977 T	19-09-1996
		EP 0467239 A	22-01-1992
		JP 4250490 A	07-09-1992

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82